

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-257670

(P 2 0 0 1 - 2 5 7 6 7 0 A)

(43) 公開日 平成13年9月21日(2001.9.21)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
H04L 9/10		G06F 12/14	320 B 5B017
G06F 12/14	320	15/00	330 Z 5B058
15/00	330	17/30	120 B 5B075
17/30	120	G06K 17/00	T 5B085
G06K 17/00		G09C 1/00	660 A 5C053

審査請求 未請求 請求項の数 4 O L (全14頁) 最終頁に続く

(21) 出願番号 特願2000-70671(P 2000-70671)

(22) 出願日 平成12年3月14日(2000.3.14)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 常広 隆司

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 片山 国弘

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100087170

弁理士 富田 和子

最終頁に続く

(54) 【発明の名称】 コンテンツ記憶装置およびコンテンツ読取装置

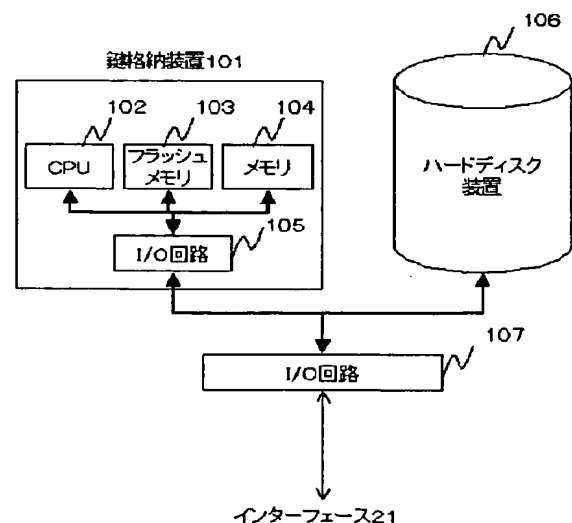
(57) 【要約】

【課題】 コンテンツ著作権などの保護を図りつつも、大量のコンテンツデータを取り扱えるようにする。

【解決手段】 コンテンツデータ毎に用意されたライセンス鍵は、暗号化されたコンテンツデータを格納するハードディスク装置106とは別個に設けられた鍵格納装置101に格納する。鍵格納装置101は通信相手の認証機能を有し、当該機能により再生装置が通信相手として認証された場合は、暗号通信を利用して当該再生装置に再生対象コンテンツデータに対応するライセンス鍵を送信する。メモリカードが通信相手として認証された場合は、暗号通信を利用して当該要求対象のライセンス鍵を送信するとともに、送信したライセンス鍵を記憶内容から消去する。

図2

コンテンツ格納装置10



【特許請求の範囲】

【請求項 1】暗号化されたコンテンツデータを記憶するコンテンツ記憶装置であって、

暗号化されたコンテンツデータを格納するコンテンツ格納手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、前記コンテンツ格納手段とは別個に設けられた計算機能付き鍵格納手段と、を有し前記計算機能付き鍵格納手段は、

通信相手を認証する認証手段を有し、

前記認証手段によりコンテンツデータの再生装置が通信相手として認証された場合に、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記認証手段により他の記憶装置が通信相手として認証された場合に、暗号通信を利用して、当該他の記憶装置へ送信すべき鍵を読み出して当該他の記憶装置へ送信するとともに、送信した鍵を記憶内容から消去することを特徴とするコンテンツ記憶装置。

【請求項 2】請求項 1 記載のコンテンツ記憶装置であって、

前記計算機能付き鍵格納手段は、

本コンテンツ記憶装置に装着自在に構成されていることを特徴とするコンテンツ記憶装置。

【請求項 3】暗号化されたコンテンツデータが記憶された可搬性を有する記憶媒体から、コンテンツデータを読み取るコンテンツ読取装置であって、

前記記憶媒体から暗号化されたコンテンツデータを読み取るコンテンツ読取手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、計算機能付き鍵格納手段と、を有し前記計算機能付き鍵格納手段は、

通信相手を認証する認証手段を有し、

前記認証手段によりコンテンツデータの再生装置が通信相手として認証された場合に、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記認証手段により他の記憶装置が通信相手として認証された場合に、暗号通信を利用して、当該他の記憶装置へ送信すべき鍵を読み出して当該他の記憶装置へ送信するとともに、送信した鍵を記憶内容から消去することを特徴とするコンテンツ読取装置。

【請求項 4】請求項 3 記載のコンテンツ読取装置であって、

前記計算機能付き鍵格納手段は、

本コンテンツ読取装置に装着自在に構成されていることを特徴とするコンテンツ読取装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、正当な権利者のみに、オーディオデータやビデオデータなどのコンテンツデータの利用を許可する技術に関し、特に、大量のコンテンツデータを取り扱うのに好適なコンテンツ記憶装置およびコンテンツ読取装置に関する。

【0002】

【従来の技術】近年、オーディオデータやビデオデータなどのコンテンツデータをネットワークを介して配信しようとする試みがなされている。たとえば、専用のメモリカードを用意し、これを販売店などに設置された専用端末に装着し、オンラインシステムを利用して所望のコンテンツデータを前記メモリカード内にダウンロードする。あるいは、専用のメモリカードを携帯電話等の個人向け端末に装着し、インターネットを利用して、コンテンツ配信センタから前記メモリカード内にダウンロードする。コンテンツデータを再生する場合には、コンテンツデータを格納した前記メモリカードを専用の再生装置に装着し、再生する。

20 【0003】

【発明が解決しようとする課題】さて、上述のような専用のメモリカードには、コンテンツデータの複製が容易であることから、コピー防止機能を設けるなどしてコンテンツ著作者などの保護を図る必要がある。

【0004】しかしながら、メモリカードでは、容量に限界があるため、大量のコンテンツデータを保存することができない。ユーザは、現在利用していないコンテンツデータであっても、コレクションとしてとっておきたい場合がある。この場合、メモリカードにコピー防止機能が付加されていると、ユーザは、メモリカードがコンテンツデータで満杯になる都度、新たなメモリカードを購入しなければならず、経済的な負担が大きい。

【0005】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、コンテンツ著作者などの保護を図りつつも、大量のコンテンツデータを取り扱うことが可能なコンテンツ記憶装置およびコンテンツ読取装置を提供することにある。

【0006】

【課題を解決するための手段】上記課題を解決するために、本発明では、コンテンツデータもしくは当該データのグループ毎に異なる鍵で暗号化されたコンテンツデータをたとえば HDD などのコンテンツ格納手段、あるいは、CD などの可搬性を有する記憶媒体に記憶する。そして、コンテンツデータもしくは当該データのグループ毎に用意された、暗号化されたコンテンツデータを復号するための鍵は、コンテンツ格納手段や記憶媒体とは別個に設けられた計算機能付き格納手段に格納しておく。

【0007】ここで、計算機能付き鍵格納手段は、通信相手を認証する認証手段を有し、当該認証手段によりコンテンツデータの再生装置が通信相手として認証された

場合は、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信する。また、当該認証手段により他の記憶装置が通信相手として認証された場合は、暗号通信を利用して、当該他の記憶装置へ送信すべき鍵を読み出して当該他の記憶装置へ送信するとともに、送信した鍵を記憶内容から消去する。

【0008】本発明において、コンテンツ格納手段あるいは可搬性を有する記憶媒体に格納されたコンテンツデータは暗号化されているので、対応する鍵がなければ復号し利用することができない。したがって、コンテンツ格納手段や記憶媒体あるいは当該媒体の読取手段に、コピー防止機能といった特別な機能を設ける必要がなくなるため、コンテンツ格納手段として一般に市販されている大容量のハードディスク装置などを利用したり、あるいは、コンテンツ読取手段として一般に市販されているCD読取装置などを利用したりすることができる。このため、大量のコンテンツデータを格納することが可能となる。

【0009】また、コンテンツ格納手段や記憶媒体に格納されたコンテンツデータを復号するためには対応する鍵が必要となるため、この鍵が計算機能付き鍵格納手段に格納されていなければ、当該コンテンツデータを復号することができない。したがって、正当な権利者（対応する鍵を有する者）のみに、コンテンツデータの再生を許可することができ、コンテンツ著作権などの保護を図ることができる。

【0010】さらに、本発明では、計算機能付き鍵格納手段に認証手段を設けている。そして、コンテンツデータの再生装置が通信相手として認証された場合、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信している。つまり、暗号化されたコンテンツデータの復号を再生装置側で行わせるようにしている。このようにすることで、鍵が外部に漏れる可能性をより低くすることができ、セキュリティを向上できる。また、他の記憶装置が通信相手として認証された場合は、送信対象の鍵を当該他の記憶装置に送信するとともに、送信した鍵を記憶内容から消去している。このようにすることで、鍵が不正にコピーされる可能性をより低くすることができ、セキュリティを向上できる。

【0011】なお、一般に、暗号化されたコンテンツデータを復号するための鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば、著しく小さい。このため、計算機能付き鍵格納手段として、本コンテンツ記憶装置あるいは読取装置に装着自在に構成された、従来の技術で説明したようなコピー防止機能を備えたメモリカードを用いた場合でも、当該メモリカードに大量のコンテンツデータに対応する鍵を格納することができるので、大量のコンテンツデータを、そのコン

テンツデータを復号する鍵とともに取り扱うことが可能となる。

【0012】

【発明の実施の形態】以下に、本発明の1実施形態について説明する。

【0013】図1は、本発明の1実施形態が適用されたコンテンツ再生装置の概略構成を示す図である。

【0014】図1において、コンテンツ格納装置10には、暗号化されたオーディオデータやビデオデータなどのコンテンツデータがそのコンテンツ名称に対応付けられて格納される。また、コンテンツ毎に用意された、暗号化されたコンテンツデータを復号するための鍵（以下、ライセンス鍵と称する）が格納される。

【0015】CPU11は、コンテンツ再生装置の各部を統括的に制御する。メモリ12は、ROMおよびRAMから構成される。ROMには、CPU11が本コンテンツ再生装置の各部を統括的に制御するためのプログラムが格納されている。RAMは、CPU11のワークエリアとして機能する。

【0016】通信装置15は、携帯電話機や据置型の電話機に接続し、オンラインシステムやインターネットなどのネットワークを介して、たとえば暗号化されたコンテンツデータやライセンス鍵を配信するコンテンツ配信センタ（不図示）にアクセスし、暗号化されたコンテンツデータやライセンス鍵を入手するのに用いられる。

【0017】入力装置16は、たとえば各種ボタンやタッチパネルで構成され、ユーザからの再生指示やコンテンツデータ、ライセンス鍵の入手指示を受け付ける。

【0018】表示装置17は、たとえば液晶パネルで構成され、コンテンツ格納装置10に格納されている暗号化されたコンテンツデータのコンテンツ名称のリストを表示したり、再生対象の暗号化されたコンテンツデータのコンテンツ名称を表示したりする。

【0019】オーディオ再生装置18は、コンテンツ格納装置10のなかから再生対象の暗号化されたオーディオデータを読み出し、これに対応するライセンス鍵を用いて復号し再生して、オーディオ信号を得る。そして、オーディオ信号を本コンテンツ再生装置に接続されたステレオに出力する。ビデオ再生装置19は、コンテンツ格納装置10のなかから再生対象の暗号化されたビデオデータを読み出し、これに対応するライセンス鍵を用いて復号し再生して、ビデオ信号を得る。そして、ビデオ信号を本コンテンツ再生装置に接続されたモニタに出力する。

【0020】カード接続装置20は、メモリカード30を接続し、当該メモリカード30から暗号化されたコンテンツデータやライセンス鍵を入手したり、当該メモリカード20へ暗号化されたコンテンツデータやライセンス鍵を送ったりする。

【0021】インターフェース21は、CPU11やメ

メモリ12と本コンテンツ再生装置を構成する他装置との間のデータ送受を司る。

【0022】次に、本コンテンツ再生装置を構成する各装置のうち、コンテンツ格納装置10、オーディオ再生装置18およびビデオ再生装置19について、さらに詳細に説明する。

【0023】まず、コンテンツ格納装置10について説明する。

【0024】図2は、コンテンツ格納装置10の概略構成を示す図である。

【0025】図示するように、コンテンツ格納装置10は、ハードディスク装置106と、鍵格納装置101と、ハードディスク装置106および鍵格納装置101がインターフェース21を介して本コンテンツ再生装置の各部とデータ送受を行うためのI/O回路107と、を備えて構成される。

【0026】ハードディスク装置10には、暗号化されたオーディオデータやビデオデータなどのコンテンツデータがそのコンテンツ名称に対応付けられて格納される。

【0027】鍵格納装置101は、CPU102と、メモリ104と、フラッシュメモリ103と、I/O回路107とのインターフェースであるI/O回路105と、を有する。

【0028】CPU102は、鍵格納装置101の各部を統括的に制御する。また、CPU102は、認証機能と暗復号化機能を有している。メモリ104は、ROMおよびRAMから構成される。ROMには、CPU102が鍵格納装置101の各部を統括的に制御するためのプログラムと、認証機能および暗復号化機能を実現するためのプログラムが格納されている。RAMは、CPU102のワークエリアとして機能する。フラッシュメモリ103には、ライセンス鍵が復号対象コンテンツのコンテンツ名称に対応付けられて格納される。ここで、ライセンス鍵は、セキュリティをより強固にするため、いわゆるタンパ・レジスタント領域 (TRM: Tamper Resistant Module) に格納するのがよい。なお、フラッシュメモリ103の代わりに、FRAMやEEPROMなどのその他の不揮発性メモリを用いることができる。

【0029】図2に示す鍵格納装置101を構成する各部は、たとえば1チップ上につくり込まれるようにしてもよいし、あるいは、複数チップで構成されるようにしてもよい。複数チップで構成する場合は、鍵格納装置101の外部からチップ間の信号を盗み取られないような工夫を施すことが好ましい。

【0030】なお、図2に示す鍵格納装置101を構成する各部は、たとえば1チップ上につくり込まれる。

【0031】次に、オーディオ再生装置18について説明する。

【0032】図3は、オーディオ再生装置18の概略構

成を示す図である。

【0033】図示するように、オーディオ再生装置18は、暗復号化回路181と、デコーダ回路182と、インターフェース21を介して本コンテンツ再生装置の各部とデータ送受を行うためのI/O回路184と、を有する。

【0034】暗復号化回路181は、コンテンツ格納装置10の鍵格納装置101から再生対象の暗号化されたオーディオデータに対応するライセンス鍵を入手し、この鍵を用いて、コンテンツ格納装置10のハードディスク装置106から読み出された再生対象の暗号化されたオーディオデータを復号する。デコーダ回路182は、暗復号化回路181で復号化されたオーディオデータを、必要に応じて伸長し、再生して、オーディオ信号を得る。そして、オーディオ信号をステレオに出力する。ここで、図3に示すオーディオ再生装置18を構成する各部は、たとえば1チップ上につくり込まれる。

【0035】次に、ビデオ再生装置19について説明する。

【0036】図4は、ビデオ再生装置19の概略構成を示す図である。

【0037】図示するように、ビデオ再生装置19は、暗復号化回路191と、デコーダ回路192と、フレームバッファ193と、インターフェース21を介して本コンテンツ再生装置の各部とデータ送受を行うためのI/O回路194とを有する。

【0038】暗復号化回路191は、コンテンツ格納装置10の鍵格納装置101から再生対象の暗号化されたビデオデータに対応するライセンス鍵を入手し、この鍵を用いて、コンテンツ格納装置10のハードディスク装置106から読み出された再生対象の暗号化されたビデオデータを復号する。デコーダ回路182は、フレームバッファ193を利用して、暗復号化回路181で復号化されたビデオデータを、必要に応じて伸長し、再生して、ビデオ信号を得る。そして、ビデオ信号をモニタに出力する。ここで、図4に示すビデオ再生装置19を構成する各部は、たとえば1チップ上につくり込まれる。

【0039】次に、本コンテンツ再生装置に装着されて用いられるメモリカード30について説明する。

【0040】メモリカード30の概略構成は、図2に示すコンテンツ格納装置10の鍵格納装置101と同じである。ただし、メモリカード30には、ライセンス鍵のみならず、暗号化されたコンテンツデータも格納されるものとする。すなわち、このメモリカード30は、たとえば販売店などに設置された専用端末に装着されて、ユーザがオンラインシステムを利用して所望の暗号化されたコンテンツデータやそのライセンス鍵を入手したり、あるいは、携帯電話等の個人向け端末に装着されて、ユーザがインターネットを利用してコンテンツ配信センタから所望の暗号化されたコンテンツデータやそのライ

ンス鍵を入手したりするのに用いることができるものとする。

【0041】ここで、図5に、本実施形態が適用されたコンテンツ再生装置の概観の一例を示す。この例のコンテンツ再生装置は、家庭内でコンテンツを楽しむのに適した据置型の形状をしている。ここで、符号41は、再生ボタン、停止ボタン、再生コンテンツ選択ボタン、および、コンテンツデータやライセンス鍵をコンテンツ格納装置10のハードディスク装置106や鍵格納装置101へ書き込んだり、カード接続装置30に接続されたメモリカード20へ移動したりするための各種設定ボタンなどで構成される操作パネルである。符号42は、操作パネル41と同じ各種ボタンを備えたりリモコン50からの指示を受け付けるための受信部である。符号43は、表示パネルであり、コンテンツ格納装置10のハードディスク装置106に格納されているコンテンツデータのコンテンツ名称のリストを表示したり、再生対象の暗号化されたコンテンツデータのコンテンツ名称を表示したりする。そして、符号44は、メモリカード30を装着するためのスロットである。図示していないが、本コンテンツ装置の背面には、モニタ51やステレオ52や携帯電話機53あるいは電話機を接続するための端子が設けられている。

【0042】次に、図6に、コンテンツ記憶装置10の概観の一例を示す。この例のコンテンツ記憶装置10は、ハードディスク装置106に鍵格納装置101を装着するためのスロットが設けられた形状をしている。ここで、符号46は、本コンテンツ格納装置10をコンテンツ再生装置のケーブル47に接続するためのコネクタであり、コンテンツ再生装置が採用するインターフェースに準拠している。符号45は、鍵格納装置101を装着するためのスロットである。鍵格納装置101には、たとえばメモリカード30と同じ構成のものを用いることができる。

【0043】なお、図5に例示するコンテンツ再生装置では、コンテンツ格納装置10を筐体内部に内蔵し、ユーザ自身が鍵格納装置101を挿抜できないようにしている。しかし、ユーザ自身がコンテンツ格納装置10の鍵格納装置10を挿抜できるように、コンテンツ格納装置10のスロット45がコンテンツ再生装置の筐体の面上にくるようにしてもかまわない。あるいは、コンテンツ格納装置10自体を挿抜できるようにするために、コンテンツ再生装置にコンテンツ格納装置10を装着するためのスロットを設けるようにしてもかまわない。

【0044】また、図6に例示するコンテンツ格納装置10では、鍵格納装置101を挿抜できるようにスロット45を設けているが、たとえば鍵格納装置101をコンテンツ格納装置10の内部に組み込んで、挿抜できないようにしてもかまわない。たとえば、鍵格納装置101をICやLSIと同じ形状のものとし、これをコンテ

ンツ格納装置10内部の基板上に設けられたソケットへ取り付けられるようにしてもかまわない。あるいは、これをコンテンツ格納装置10内部の基板に直接半田付けするようにしてもかまわない。

【0045】次に、本実施形態のコンテンツ再生装置の動作について説明する。

【0046】まず、コンテンツデータを再生する場合の動作について説明する。

【0047】図7は、本実施形態が適用されたコンテンツ再生装置の再生動作を説明するためのフロー図である。このフローは、たとえば、ユーザが入力装置16を用いて、表示装置17に表示されている、コンテンツ格納装置10のハードディスク装置106に格納されているコンテンツデータのコンテンツ名称のリストの中から、再生対象のコンテンツを選択し、再生指示を入力すると開始される。

【0048】まず、CPU11は、入力装置16を介してユーザより受け付けたコンテンツデータの再生指示を、当該コンテンツデータの種類（オーディオデータ/ビデオデータ）を再生するオーディオ再生装置18/ビデオ再生装置19に送信する（S1001）。

【0049】CPU11より再生指示を受け取ったオーディオ再生装置18/ビデオ再生装置19の暗復号化回路181/191は、自身の認証データと再生対象の暗号化されたコンテンツデータの識別情報（たとえばコンテンツ名称）を含んだ、当該コンテンツデータ再生のためのライセンス鍵送信指示を、コンテンツ格納装置10の鍵格納装置101に送信する（S1002）。

【0050】鍵格納装置101のCPU102は、コンテンツデータ再生のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う（S1003）。たとえば、認証データが予め本鍵格納装置101に登録されているオーディオ/ビデオ再生装置であることを示しているか否かを調べる。そして、当該指示の送信元がオーディオ再生装置18/ビデオ再生装置19であることを認証したならば（S1004でYesの場合）、当該指示に含まれる識別情報により特定されるコンテンツデータのライセンス鍵がフラッシュメモリ103に格納されているか否かを調べる（S1005）。格納されていれば（S1006でYesの場合）、そのライセンス鍵をフラッシュメモリ103から読み出し、暗号通信を利用して、当該指示の送信元であるオーディオ再生装置18/ビデオ再生装置19に送信する（S1008）。

【0051】なお、S1004において指示の送信元がオーディオ再生装置18/ビデオ再生装置19であることを認証できなかった場合、および、S1006において所望のライセンス鍵がフラッシュメモリ103に格納されていなかった場合、鍵格納装置101のCPU102は、CPU11にその旨伝える。これを受けて、CP

U11は表示装置17にエラー表示を行うなど、所定のエラー処理を行う(S1007)。

【0052】さて、コンテンツデータ再生のためのライセンス鍵送信指示を送信したオーディオ再生装置18/ビデオ再生装置19の暗複号化回路181/191は、コンテンツ格納装置10の鍵格納装置101からライセンス鍵を受け取ると、コンテンツ格納装置10のハードディスク装置106から再生対象の暗号化されたコンテンツデータを読み出す(S1009)。そして、これをライセンス鍵で復号して、デコーダ回路182/192に渡す。デコーダ回路182/192は、暗複号化回路181/191から受け取ったコンテンツデータを必要に応じて伸長し、再生してオーディオ/ビデオデータを得、ステレオ/モニタに出力する(S1010)。

【0053】次に、図7に示すフローにおける鍵格納装置101およびオーディオ再生装置18/ビデオ再生装置19間のデータのやり取りについて、その一例を説明する。

【0054】図8は、図7に示すフローにおける鍵格納装置101およびオーディオ再生装置18/ビデオ再生装置19間のデータのやり取りの一例を説明するためのシーケンス図である。

【0055】オーディオ再生装置18/ビデオ再生装置19の暗複号化回路181/191は、図7のS1002において、自身の認証データと、再生対象の暗号化されたコンテンツデータの識別情報と、予め保持しているメディアクラス秘密鍵 $K_{r,c}$ と対のメディアクラス公開鍵 $K_{o,c}$ とを含んだライセンス鍵送信指示を作成し、これをコンテンツ格納装置10の鍵格納装置101に送信する(T1001)。

【0056】これを受けて、鍵格納装置101のCPU102は、図7のS1004~S1007において、オーディオ再生装置18/ビデオ再生装置19の認証、および、フラッシュメモリ103に要求されたライセンス鍵が格納されていることの確認を行う(T1002)。それから、CPU102は、セッション鍵 K_s を生成し(T1003)、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵 $K_{o,c}$ で暗号化して、当該指示の送信元であるオーディオ再生装置18/ビデオ再生装置19に送信する(T1004)。

【0057】これを受けて、オーディオ再生装置18/ビデオ再生装置19の暗複号化回路181/191は、暗号化されたセッション鍵 K_s を予め保持しているメディアクラス秘密鍵 $K_{r,c}$ で復号し、セッション鍵 K_s を得る(T1005)。それから、乱数 K_z を生成し(T1006)、これと、予め保持しているメディア固有秘密鍵 K_r と対のメディア固有公開鍵 K_o とを、セッション鍵 K_s で暗号化して、コンテンツ格納装置10の鍵格納装置101に送信する(T1007)。

【0058】これを受けて、鍵格納装置101のCPU

102は、暗号化された乱数 K_z とメディア固有公開鍵 K_o とを、セッション鍵 K_s で復号し、乱数 K_z とメディア固有公開鍵 K_o を得る(T1008)。そして、送信を要求されているライセンス鍵 K_c をメディア固有公開鍵 K_o で暗号化し、さらにこれを乱数 K_z で暗号化して、ライセンス鍵送信指示の送信元であるオーディオ再生装置18/ビデオ再生装置19に送信する(T1009)。

【0059】これを受けて、オーディオ再生装置18/ビデオ再生装置19の暗複号化回路181/191は、暗号化されたライセンス鍵 K_c を乱数 K_z とメディア固有秘密鍵 K_r を用いて復号し、ライセンス鍵 K_c を得る(T1010)。

【0060】以上、コンテンツデータを再生する場合の動作について説明した。

【0061】次に、メモリカード30からライセンス鍵を入手する場合の動作について説明する。

【0062】図9は、本実施形態が適用されたコンテンツ再生装置に接続されたメモリカード30からライセンス鍵を入手する場合の動作を説明するためのフロー図である。このフローは、たとえば、本コンテンツ再生装置にメモリカード30が装着された状態で、ユーザが入力装置16を用いて、表示装置17に表示されている、メモリカード30に格納されているライセンス鍵に対応するコンテンツ名称のリストのなかから、入手対象のライセンス鍵に対応するコンテンツを選択し、ライセンス鍵入手指示を入力すると開始される。

【0063】まず、CPU11は、入力装置16を介してユーザよりライセンス鍵入手指示を受け付けたならば、その旨をコンテンツ格納装置の鍵格納装置101に送信する(S2001)。

【0064】CPU11よりライセンス鍵入手指示を受け取った鍵格納装置101のCPU102は、自身の認証データと入手対象のライセンス鍵の識別情報(たとえば当該鍵で復号可能なコンテンツ名称)を含んだ、当該ライセンス鍵入手のためのライセンス鍵送信指示を、カード接続装置20に接続されたメモリカード30に送信する(S2002)。

【0065】メモリカード30のCPUは、ライセンス鍵入手のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う(S2003)。たとえば、認証データが予め本メモリカード30に登録されている鍵格納装置であることを示しているか否かを調べる。そして、当該指示の送信元が鍵格納装置101であることを認証したならば(S2004でYesの場合)、当該指示に含まれる識別情報により特定されるライセンス鍵がメモリカード30内に格納されているか否かを調べる(S2005)。格納されていれば(S2006でYesの場合)、そのライセンス鍵を読み出し、暗号通信を利用して、当該指示の送信

元であるコンテンツ格納装置10の鍵格納装置101に送信する(S2008)。それから、送信したライセンス鍵をメモリカード30内から消去する(S2009)。

【0066】なお、S2004において指示の送信元が鍵格納装置101であることを認証できなかった場合、および、S2006において所望のライセンス鍵がメモリカード30内に格納されていなかった場合、メモリカード30のCPUは、CPU11にその旨伝える。これを受けて、CPU11は表示装置17にエラー表示を行うなど、所定のエラー処理を行う(S2007)。

【0067】さて、ライセンス鍵入手のためのライセンス鍵送信指示を送信した鍵格納装置101のCPU102は、カード接続装置20に接続されたメモリカード30からライセンス鍵を受け取ると、これをたとえば当該鍵で復号可能なコンテンツデータのコンテンツ名称に対応付けてフラッシュメモリ103に格納する(S2010)。

【0068】次に、図9に示すフローにおける鍵格納装置101およびメモリカード30間のデータのやり取りについて、その一例を説明する。

【0069】図10は、図9に示すフローにおける鍵格納装置101およびメモリカード30間のデータのやり取りの一例を説明するためのシーケンス図である。

【0070】コンテンツ格納装置10の鍵格納装置101のCPU102は、図9のS2002において、自身の認証データと、入手対象のライセンス鍵の識別情報と、予め保持しているメディアクラス秘密鍵 K'_{rc} と対のメディアクラス公開鍵 K'_{rc} とを含んだライセンス鍵送信指示を作成し、これをメモリカード30に送信する(T2001)。

【0071】これを受けて、メモリカード30のCPUは、図9のS2004～S2007において、鍵格納装置101の認証、および、メモリカード30内に要求されたライセンス鍵が格納されていることの確認を行う(T2002)。それから、メモリカード30のCPUは、セッション鍵 K_s を生成し(T2003)、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵 K'_{rc} で暗号化して、当該指示の送信元であるコンテンツ格納装置10の鍵格納装置101に送信する(T2004)。

【0072】これを受けて、鍵格納装置101のCPU102は、暗号化されたセッション鍵 K_s を予め保持しているメディアクラス秘密鍵 K'_{rc} で復号し、セッション鍵 K_s を得る(T2005)。それから、乱数 K_r を生成し(T2006)、これと、予め保持しているメディア固有秘密鍵 K'_{rv} と対のメディア固有公開鍵 K'_{rv} とを、セッション鍵 K_s で暗号化して、メモリカード30に送信する(T2007)。

【0073】これを受けて、メモリカード30のCPU

は、暗号化された乱数 K_r とメディア固有公開鍵 K'_{rv} を、セッション鍵 K_s で復号し、乱数 K_r とメディア固有公開鍵 K'_{rv} を得る(T2008)。そして、送信を要求されているライセンス鍵 K_c をメディア固有公開鍵 K'_{rv} で暗号化し、さらにこれを乱数 K_r で暗号化して、ライセンス鍵送信指示の送信元であるコンテンツ格納装置10の鍵格納装置101に送信する(T2009)。

【0074】これを受けて、鍵格納装置101のCPU102は、暗号化されたライセンス鍵 K_c を乱数 K_r とメディア固有秘密鍵 K'_{rv} を用いて復号し、ライセンス鍵 K_c を得る(T2010)。

【0075】以上、メモリカード30からライセンス鍵を入手する場合の動作について説明した。

【0076】次に、コンテンツ格納装置10の鍵格納装置101に格納されているライセンス鍵をメモリカード30へ移動する場合の動作について説明する。

【0077】図11は、本実施形態が適用されたコンテンツ再生装置のコンテンツ格納装置10の鍵格納装置101から、本コンテンツ再生装置に接続されたメモリカード30へライセンス鍵を移動する場合の動作を説明するためのフロー図である。このフローは、たとえば、本コンテンツ再生装置にメモリカード30が装着された状態で、ユーザが入力装置16を用いて、表示装置17に表示された、コンテンツ格納装置10の鍵格納装置101に格納されているライセンス鍵に対応するコンテンツ名称のリストのなかから、移動対象のライセンス鍵に対応するコンテンツを選択し、ライセンス鍵移動指示を入力すると開始される。

【0078】まず、CPU11は、入力装置16を介してユーザよりライセンス鍵移動指示を受け付けたならば、その旨をメモリカード30に送信する(S3001)。

【0079】CPU11よりライセンス鍵移動指示を受け取ったメモリカード30のCPUは、自身の認証データと移動対象のライセンス鍵の識別情報(たとえば当該鍵で復号可能なコンテンツ名称)を含んだ、当該ライセンス鍵移動のためのライセンス鍵送信指示を、コンテンツ格納装置10の鍵格納装置101に送信する(S3002)。

【0080】鍵格納装置101のCPU102は、ライセンス鍵移動のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う(S3003)。たとえば、認証データが予め本鍵格納装置101に登録されているメモリカードであることを示しているか否かを調べる。そして、当該指示の送信元がメモリカード30であることを認証したならば(S3004でYesの場合)、当該指示に含まれる識別情報により特定されるライセンス鍵がフラッシュメモリ103内に格納されているか否かを調べる(S300

5)。格納されていれば(S3006でYesの場合)、そのライセンス鍵を読み出し、暗号通信を利用して、当該指示の送信元であるメモリカード30に送信する(S3008)。それから、送信したライセンス鍵をフラッシュメモリ103内から消去する(S3009)。

【0081】なお、S3004において指示の送信元がメモリカード30であることを認証できなかった場合、および、S3006において所望のライセンス鍵がフラッシュメモリ103内に格納されていなかった場合、鍵格納装置101のCPU102は、CPU11にその旨伝える。これを受けて、CPU11は表示装置17にエラー表示を行うなど、所定のエラー処理を行う(S3007)。

【0082】さて、ライセンス鍵移動のためのライセンス鍵送信指示を送信したメモリカード30のCPUは、鍵格納装置101からライセンス鍵を受け取ると、これをたとえば当該鍵で復号可能なコンテンツデータのコンテンツ名称に対応付けてメモリカード30内に格納する(S3010)。

【0083】なお、図11に示すフローにおける鍵格納装置101およびメモリカード30間のデータのやり取りは、図10に示すシーケンス図において、鍵格納装置101およびメモリカード30の動作を互いに交換したものとなる。

【0084】以上、メモリカード30へライセンス鍵を移動する場合の動作について説明した。

【0085】なお、通信装置15に接続された携帯電話機/据置型電話機を利用して、オンラインシステムやインターネットなどのネットワークを介して、コンテンツ配信センタ(不図示)からライセンス鍵を入手する場合の動作は、一般的な、ネットワークを介したデータダウンロードと同じものでよい。ただし、正当な権利を有する者のみがライセンス鍵を入手できるようにするために、コンテンツ格納装置10の鍵格納装置101とコンテンツ配信センタとの間で認証処理を行い、コンテンツ配信センタが鍵格納装置101を認証した場合にのみ、ライセンス鍵のダウンロードを許可するようにすることが好ましい。また、コンテンツデータのコンテンツ格納装置10のハードディスク装置106へのダウンロードは、たとえば、メモリカード30に格納されたコンテンツデータをコピーしてハードディスク装置106に格納するようにしてもよいし、あるいは、通信装置15に接続された携帯電話機/据置型電話機を利用して、オンラインシステムやインターネットなどのネットワークを介して、コンテンツ配信センタ(不図示)から入手し、ハードディスク装置106に格納するようにしてもよい。いずれにしても、コンテンツデータは暗号化されており、対応するライセンス鍵がなければ復号・再生できない。

【0086】以上、本発明の1実施形態について説明した。

【0087】本実施形態において、コンテンツ格納装置10のハードディスク装置106に格納されたコンテンツデータは暗号化されているので、対応するライセンス鍵がなければ復号し再生することができない。したがって、ハードディスク装置106にコピー防止機能といった特別な機能を設ける必要がなくなるため、ハードディスク装置106として、一般に市販されている大容量のハードディスクドライブを利用でき、大量のコンテンツデータを格納することが可能となる。

【0088】また、コンテンツ格納装置10のハードディスク装置106に格納されたコンテンツデータを復号するためには対応するライセンス鍵が必要となるため、このライセンス鍵がコンテンツ格納装置10の鍵格納装置101に格納されていなければ、当該コンテンツデータを再生することができない。したがって、正当な権利者(対応するライセンス鍵を有する者)のみに、コンテンツデータの再生を許可することができ、コンテンツ著作権者などの保護を図ることができる。

【0089】さらに、本実施形態では、暗号化されたコンテンツデータの復号を、コンテンツデータの再生を行うオーディオ再生装置18/ビデオ再生装置19で行うようにしている。そして、コンテンツ格納装置10の鍵格納装置101は、ライセンス鍵の送信相手がオーディオ再生装置18/ビデオ再生装置1であることを認証した場合に、当該ライセンス鍵を暗号通信を利用してオーディオ再生装置18/ビデオ再生装置19に送るようにしている。このようにすることで、ライセンス鍵が外部に漏れる可能性をより低くすることができ、セキュリティを向上できる。

【0090】くわえて、本実施形態において、コンテンツ格納装置10の鍵格納装置101は、ライセンス鍵の送信相手がメモリカード30である場合、送信したライセンス鍵を鍵格納装置101の記憶内容から消去するようにしている。つまり、鍵格納装置101にライセンス鍵のコピー防止機能を設けている。このようにすることで、ライセンス鍵が不正にコピーされる可能性を減らすことができる。

【0091】なお、一般に、鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば、著しく小さい。このため、鍵格納装置101の記憶部をフラッシュメモリ103で構成した場合でも、当該フラッシュメモリ103に多くのライセンス鍵を格納することができる。したがって、家のなかでコンテンツデータの再生を楽しむような据置型に適したコンテンツ再生装置を提供できる。

【0092】なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【0093】たとえば、上記の実施形態では、暗号化されたコンテンツデータがコンテンツ格納装置 10 のハードディスク装置 106 に格納されている場合を例に取り説明した。しかしながら、本発明はこれに限定されるものではない。暗号化されたコンテンツデータは、CD などの可搬性を有する記憶媒体に格納された形態で提供されるものでもよい。この場合、本実施形態において、コンテンツ格納装置 10 のハードディスク装置 106 に代えて、前記可搬性を有する記憶媒体から暗号化されたコンテンツデータを読み取る読取装置を設けるようにすればよい。

【0094】また、上記の実施形態では、ライセンス鍵を暗号化されたコンテンツデータ毎に用意しているが、本発明はこれに限定されない。たとえば、複数の暗号化されたコンテンツデータを 1 グループとして、グループ毎に、当該グループに属する暗号化されたコンテンツデータを復号するためのライセンス鍵を用意するようにしてもよい。

【0095】

【発明の効果】以上説明したように、本発明によれば、コンテンツ著作権などの保護を図りつつも、大量のコンテンツデータを取り扱うことが可能となる。

【図面の簡単な説明】

【図 1】本発明の 1 実施形態が適用されたコンテンツ再生装置の概略構成を示す図である。

【図 2】図 1 に示すコンテンツ格納装置 10 の概略構成を示す図である。

【図 3】図 1 に示すオーディオ再生装置 18 の概略構成を示す図である。

【図 4】図 1 に示すビデオ再生装置 19 の概略構成を示す図である。

【図 5】本発明の 1 実施形態が適用されたコンテンツ再生装置の概観の一例を示す図である。

【図 6】図 2 に示すコンテンツ格納装置 10 の概観の一例を示す図である。

【図 7】本発明の第 1 実施形態が適用されたコンテンツ再生装置の再生動作を説明するためのフロー図である。

【図 8】図 7 に示すフローにおけるコンテンツ格納装置 10 の鍵格納装置 101 およびオーディオ再生装置 18 / ビデオ再生装置 19 間のデータのやり取りの一例を説

明するためのシーケンス図である。

【図 9】本発明の第 1 実施形態が適用されたコンテンツ再生装置に接続されたメモリカード 30 からライセンス鍵を入手する場合の動作を説明するためのフロー図である。

【図 10】図 9 に示すフローにおけるコンテンツ格納装置 10 の鍵格納装置 101 およびメモリカード 30 間のデータのやり取りの一例を説明するためのシーケンス図である。

【図 11】本発明の 1 実施形態が適用されたコンテンツ再生装置のコンテンツ格納装置 10 の鍵格納装置 101 から本コンテンツ再生装置に接続されたメモリカード 30 へライセンス鍵を移動する場合の動作を説明するためのフロー図である。

【符号の説明】

11、102…CPU

12、104…メモリ

10…コンテンツ格納装置

15…通信装置

16…入力装置

17…表示装置

18…オーディオ再生装置

19…ビデオ再生装置

20…カード接続装置

21…インターフェース

30…メモリカード

41…操作パネル

42…受信部

43…表示パネル

44、45…スロット

46…コネクタ

50…リモコン

51…モニタ

52…ステレオ

53…携帯電話機

103…フラッシュメモリ

105、107、184、194…I/O回路

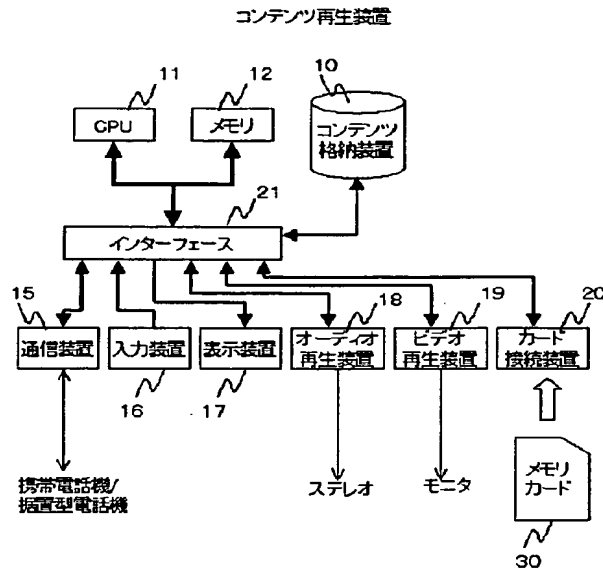
181、191…暗復号化回路

182、192…デコーダ回路

193…フレームバッファ

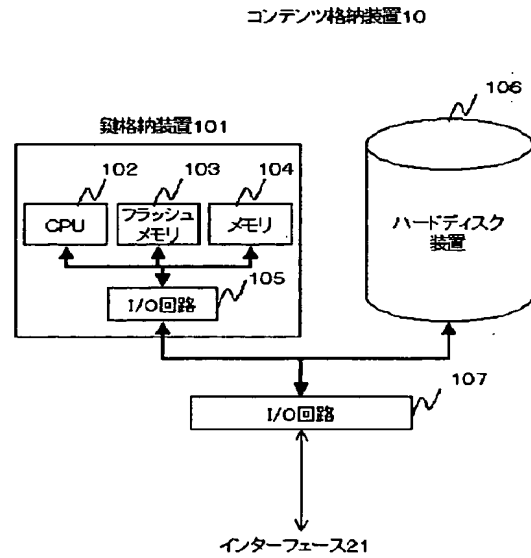
【図 1】

図1



【図 2】

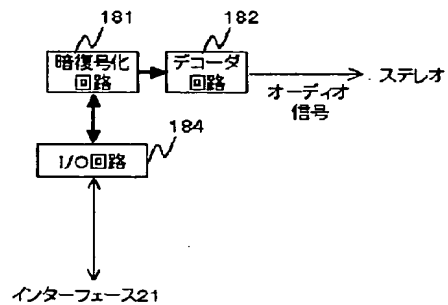
図2



【図 3】

図3

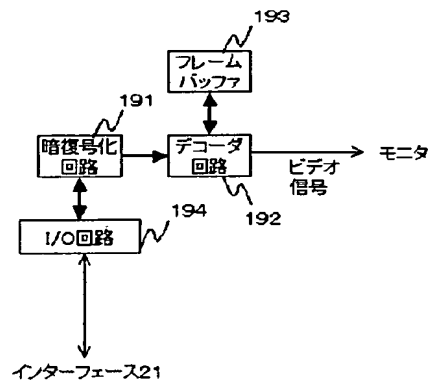
オーディオ再生装置18



【図 4】

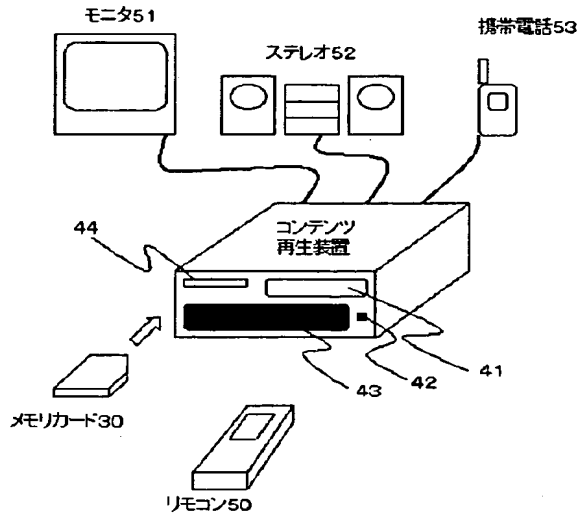
図4

ビデオ再生装置19



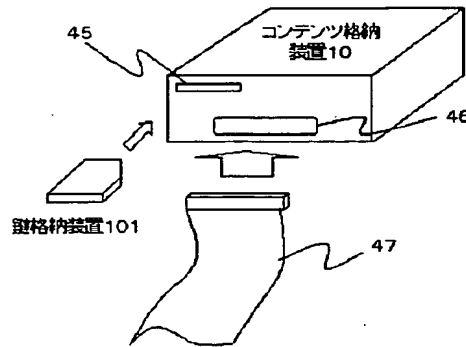
【図5】

図5



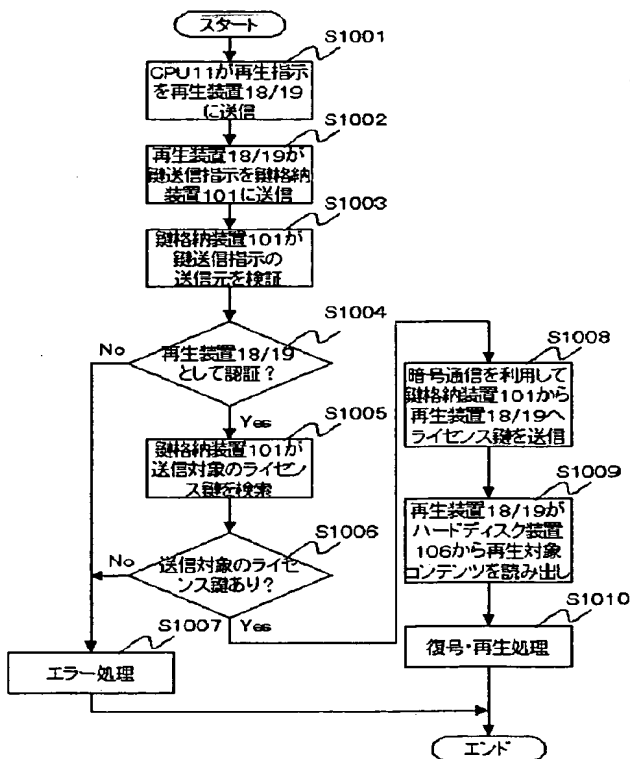
【図6】

図6



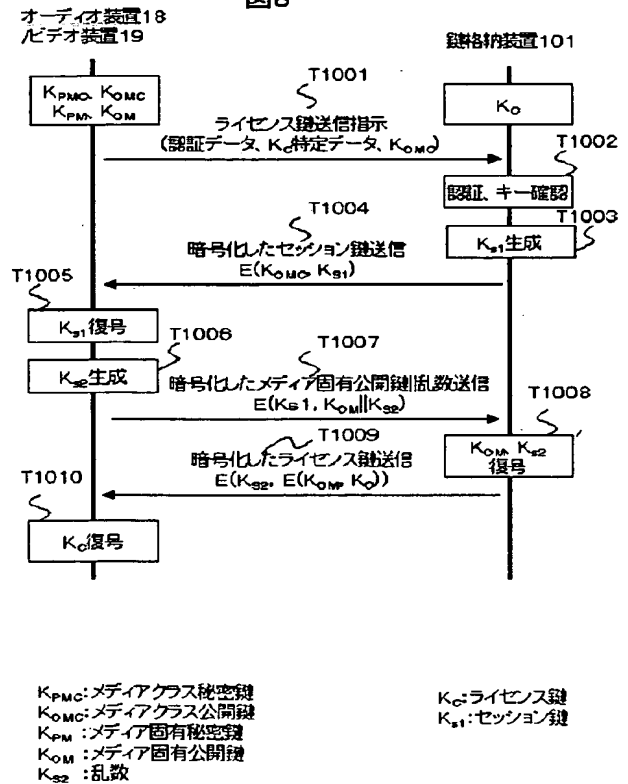
【図7】

図7

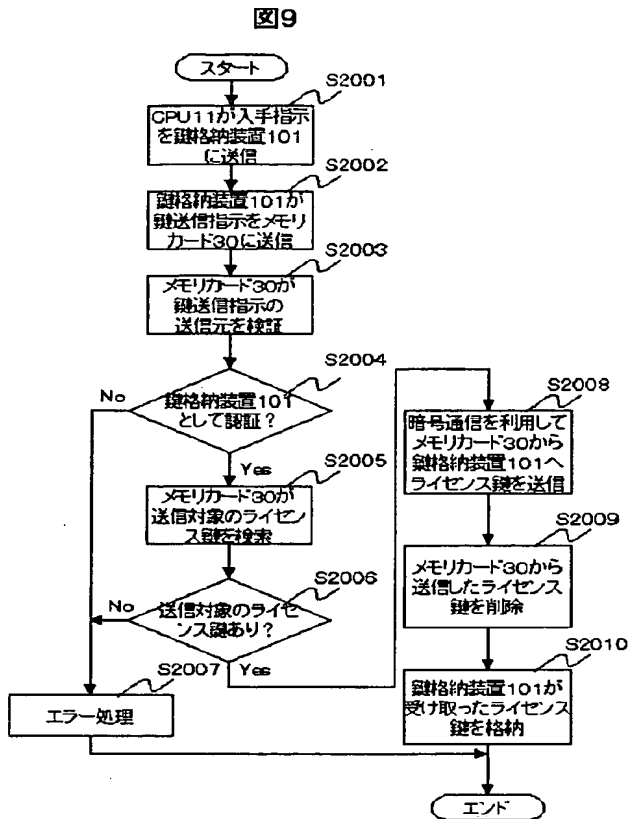


【図8】

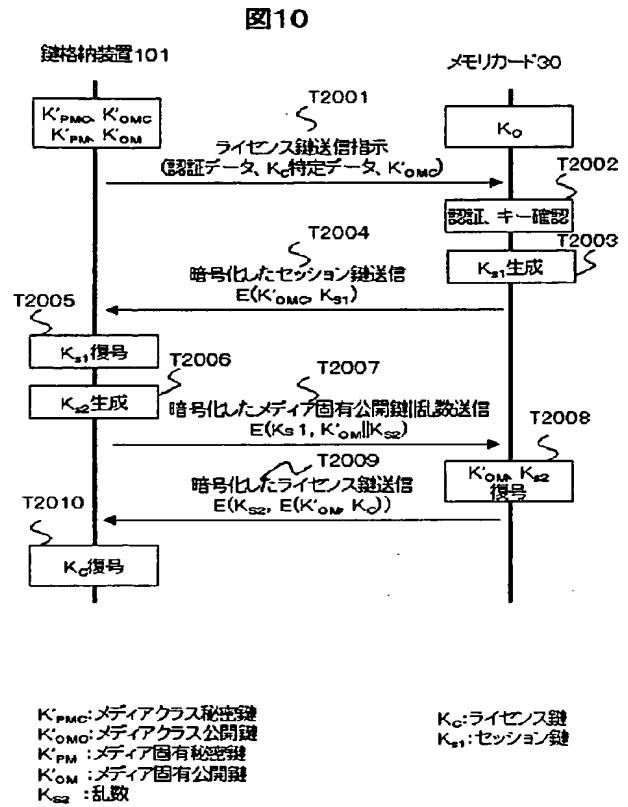
図8



【図 9】

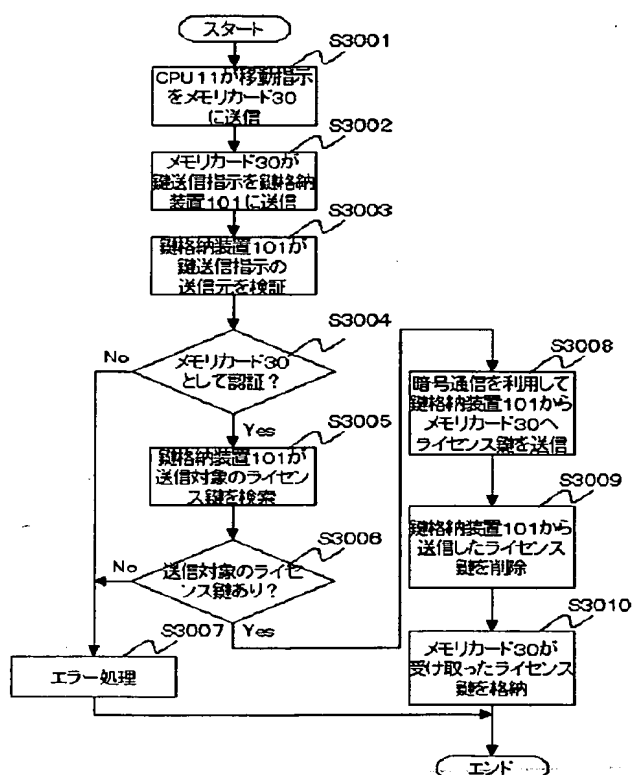


【図 10】



【図11】

図11



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	ターマコード (参考)
G09C 1/00	660	G11B 20/10	H 5C064
G11B 20/10		H04L 9/00	621 A 5D044
H04N 5/91		H04N 5/91	P 5J104
7/167		7/167	Z 9A001

- (72)発明者 水島 永雅
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内
- (72)発明者 角田 元泰
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内
- (72)発明者 白石 和久
神奈川県小田原市国府津2880番地 株式会社日立製作所ストレージシステム事業部内
- (72)発明者 戸塚 隆
東京都小平市上水本町五丁目20番1号 株式会社日立製作所半導体グループ内

- (72)発明者 ▲真▼野 宏之
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内
- (72)発明者 中村 一男
東京都小平市上水本町五丁目20番1号 株式会社日立製作所半導体グループ内

Fターム(参考) 5B017 AA06 BA07 BB03 CA07 CA14
CA16
5B058 KA01 KA04 KA06 KA33 KA35
5B075 KK07 KK50 KK54 KK63 KK68
MM01 MM11 MM23 ND16 UU37
5B085 AA01 AE00 AE09 AE29 BE01
5C053 FA13 FA15 FA23 FA27 FA29
GA11 GB21 JA01 JA21 KA24
LA11 LA14
5C064 CA14 CB01 CC02 CC04
5D044 AB05 AB07 CC08 DE50 DE53
DE58 GK12 GK17 HL08
5J104 AA12 EA06 EA09 EA18 EA19
KA02 NA02 NA03 NA35 NA37
9A001 BB03 EE03 JZ67 KK62 LL03